

WHITE PAPER



PRESENTED BY:



VULNERABILITY MANAGEMENT:

HOW VULNERABILITY MANAGEMENT CONTRIBUTES TO THE SECURITY OF INFORMATION TECHNOLOGY SYSTEMS AND ENTERPRISE BUSINESS FUNCTIONS

David Shay, ISSE

James D. Heimberg, ABC, Ph.D., ISSO

May 9, 2006

INTRODUCTION

Federal Network Services, Inc., Information Security (INFOSEC) Services practice is pleased to present this white paper that describes how establishing a comprehensive vulnerability management capability including vulnerability identification, fixing and/or remediating of those vulnerabilities, and on-going awareness of newly discovered vulnerabilities in IT products contributes to the security and overall continued functionality of business support functions of an Information Technology (IT) system, network, or operational environment.

From July 2003 through June 2005, the average number of published computer vulnerabilities was more than 2500 per year, or nearly seven each day. Even a small organization with a single server can expect to spend time reviewing a handful of critical patches every month. This stream of vulnerabilities has resulted in systems constantly being threatened by new attacks.

The level of damage caused by an attack can be quite severe. A number of Internet worms (self-propagating code that exploits vulnerabilities over the Internet) such as Code Red, Nimda, Blaster, and MyDoom have been released in recent years. There are some common data points for these worm outbreaks. First, as worm code authors have gotten more sophisticated, the worms have spread faster than their predecessors. Second, the worms each hit hundreds of thousands of computers worldwide. Most importantly, each one of them attacked a known vulnerability for which a patch or other mitigation steps had already been released. Each major outbreak was preventable.

The INFOSEC Services practice prepared this white paper to describe how it can develop and deliver a complete suite of vulnerability management consulting and technical support services to help its clients establish and operate a viable program. INFOSEC Services offers security professionals, infrastructure consulting, and development services that are among the best in the industry, and an array of IT products that support establishment and operation of a secure IT infrastructure. Our vulnerability management tools include:

- Eraser
- LanMapShot
- Microsoft Visio
- PCAnywhere
- Whisker
- Hyena
- LOphtcrack
- STAT Analyzer
- ISS Scanner
- Stryker/Auditor-Lockdown Networks
- HP Radia
- Nessus
- PGP Disk
- Netstumbler
- KillDisk
- Net Recon
- Windows2000 KeyLog
- Linux Keystroke Logger
- Norton products
- MacAfee products

This paper identifies the major components of vulnerability management program, raises a few practical issues that must be addressed when implementing such a program, and discusses decision points that need to be addressed when establishing such a capability.

VULNERABILITY MANAGEMENT – DEFINED

Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization. The expected result is to reduce the time and money spent dealing with vulnerabilities and exploitation of those vulnerabilities. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after exploitation.

A key process for managing vulnerabilities involves the deployment of patches and software updates throughout the enterprise. Patches are additional pieces of code developed to address problems (commonly called “bugs”) in software. Patches enable additional functionality or address security flaws within a program. Vulnerabilities are flaws that can be exploited by a

malicious entity to gain greater access or privileges than it is authorized to have on a computer system. Most successful attacks exploit known problems in software that have not been patched or updated. However, not all vulnerabilities have related patches; thus, system administrators must not only be aware of applicable vulnerabilities and available patches, but also other methods of remediation (e.g., device or network configuration changes, employee training) that limit the exposure of systems to vulnerabilities.

In summary:

- **Vulnerabilities** – Vulnerabilities are software flaws or misconfigurations that result in weaknesses in the security of a system. Vulnerabilities can be exploited by a malicious entity to violate policies—for example, to gain greater access or permission than is authorized on a computer.
- **Remediation** – There are three primary methods of remediation: installation of a software patch, adjustment of a configuration setting, and removal of affected software.
- **Threats** – Threats are capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and potentially cause harm to a computer system or network. Threats usually take the form of exploit scripts, worms, viruses, rootkits, and Trojan horses.
- **Vulnerability Assessment** – Systematic examination of networks to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. The measures are also called Network Vulnerability Assessment, Network Vulnerability, Security Vulnerabilities, Network Security Vulnerabilities, Vulnerabilities, Host Vulnerability Assessment, Vulnerability Management, and Internet Security Vulnerabilities

BUSINESS DRIVERS, ISSUES AND CONSIDERATIONS

It is important for an organization to know how quickly it can identify, analyze, and respond to a new vulnerability and to mitigate the potential impact of a successful attack based on that vulnerability. Response time has become increasingly important, because the average time between a vulnerability announcement and an exploit being released has decreased dramatically in the last few years. There are three primary response time measurements that can be taken: vulnerability and patch identification, patch application, and emergency security configuration changes or actions (such as shutting down a process or access thereto).

RESPONSE TIME FOR VULNERABILITY AND PATCH IDENTIFICATION

This is how long it takes vulnerability management professionals to learn about a new vulnerability or patch. Timing begins from the moment the vulnerability or patch is publicly known. This measurement should be taken on a sampling of different patches and vulnerabilities and should include all of the different resources the professionals use to gather information.

RESPONSE TIME FOR PATCH APPLICATION

This is how long it takes to apply a patch to all relevant IT devices within the system. Timing begins from the moment the vulnerability management team becomes aware of a patch. This measurement should be taken on patches where it is relatively easy for the professionals to verify patch installation. This measurement includes the time spent for:

- Patch analysis
- Patch testing
- Configuration management process
- Patch deployment effort

Verification can be done through the use of enterprise patch management tools or through vulnerability scanning (both host and network-based). It is useful to take this measurement on both critical and noncritical security patches, since a different process is usually used by enterprises in both cases, and the timing will likely be different.

RESPONSE TIME FOR EMERGENCY CONFIGURATION CHANGES

This applies in situations where a vulnerability exists that must be mitigated but where there is no patch. In such cases, the organization is forced to make emergency configuration changes that may reduce functionality to protect the organization from exploitation of the vulnerability. Such changes are often done at the firewall, e-mail server, Web server, central file server, or servers in the Demilitarized Zone (DMZ). The changes may include turning off or filtering certain e-mail attachments, e-mail subjects, network ports, and server applications. The organization needs to know the time it takes from the moment the enterprises' vulnerability professionals learn about the vulnerability to the moment that an acceptable workaround has been applied and verified.

These activities are normally done on an emergency basis, so obtaining a reasonable measurement sample size may be difficult. Given the importance of determining the response time for emergency situations, these emergency processes should be tested regularly. The following list identifies examples of emergency processes should be tested and timed.

- Firewall or router configuration change
- Network disconnection
- Intrusion prevention device activation or reconfiguration
- E-mail filtering rules addition
- Computer isolation
- Emergency notification of staff

As much as possible, enterprises should create standard system emergency processes, which will help make the testing results more uniform. Enterprises should capture and review the metrics following any emergency configuration change as a part of an operational debriefing to determine subsequent actions and areas for improvement in the emergency change process.

COST AND RETURN-ON-INVESTMENT DECISIONS

For an organization to make decisions on where and how much to invest in protecting its information and IT components, it needs to identify the costs of vulnerability management components as well as the potential losses if prudent safeguards and protection mechanisms are not implemented. The discussion below provides a starting point for making, often difficult business decisions for vulnerability management.

Cost of the Patch and Vulnerability Group

Measuring the cost of patch and vulnerability management is difficult because the actions are often split between different people in various groups. In the simplest case, there will be a dedicated centralized team that deploys patches and security configurations directly. Some organizations will have patch and vulnerability functions split between multiple groups. There are four main cost measurements that should be considered and each is discussed below.

This information is easy to obtain since the people involved in vulnerability management are easily identifiable. Some organizations outsource significant parts of their vulnerability management functions, and the cost of this outsourcing should be included in the analysis.

Cost of System Administrator Support

This element is difficult to determine with accuracy. The main problem is that, historically, system administrators have not been asked to calculate the amount of time they spend on security, much less on security patch and vulnerability management. As organizations improve in their overall efforts to measure the real cost of IT security, measuring the cost of patch and vulnerability measurement with respect to system administrator time is becoming easier.

Cost of Enterprise Patch and Vulnerability Management Tool

This includes the cost of patching tools, vulnerability scanning tools, vulnerability Web portals, vulnerability databases, and log analysis tools (used for verifying patches). It should not include intrusion detection, intrusion prevention, and log analysis tools (used for intrusion detection).

Cost of Program Failures

This requires that an estimate be made of the total cost of the business impact of all incidents that could have been prevented if the patch and vulnerability mitigation program had been more effective, as well as all problems caused by the patching process itself, such as a patch inadvertently breaking an application. The cost analysis normally includes tangible losses (e.g., worker time and destroyed data) as well as intangibles (e.g., placing a value on an organization's reputation). If the cost of program failures is extremely high, then the organization may be able to save money by investing more resources in their vulnerability management program. If the cost of program failures is extremely low, then the organization can maintain the existing level of support for vulnerability management or possibly even decrease it slightly to optimize cost effectiveness.

SUPPORTING CERTIFICATION AND ACCREDITATION

The Certification and Accreditation (C&A) process requires that a viable vulnerability and threat monitoring capability be established and maintained throughout the life of a system. System administrators should monitor for vulnerabilities, remediation, and threats for systems under their control.

Every Federally owned system currently is mandated by law to have vulnerability analyses completed at regular intervals with some interval set for third-party testing. Most often, the vulnerability evaluation must be provided in quarterly reports to a higher-level authority for inclusion in the overall management evaluation of the organization. This is the case when vulnerability test results are reported under the Federal Information System Management Act (FISMA). In the C&A documents, the vulnerabilities should be fully described in a manner that allows translation to the FISMA required reports, such as the Plan of Action and Milestones (POA&M). Thus, vulnerability test and management become key components in building C&A documentation.

Once data about the system, data protection, and *vulnerabilities* are brought together, an evaluation of risk can be accomplished. Thus, identification of vulnerabilities and potential remediation, including identification of costs for each is an essential step in the overall C&A process for Federal agencies. Federal mandates are expected to be levied on local and state governments and some parts of industry as well in the near future. Likewise, in a commercial industry setting, identification and analysis of vulnerabilities and remediation process and the costs applicable thereto is a necessary step in the preparation of data for decision makers who must determine how much and where to invest in preventive protection technologies and staff resources for safeguarding enterprise information resources and IT assets.

BEST PRACTICES

Vulnerability management is a process that can be implemented to make IT environments more secure and to improve an organization's regulatory compliance posture. Industry and government best practice for an effective vulnerability management program includes the following essential elements:

- Policy definition – The first step includes defining the desired state for device configurations, user identity and resource access
- Baseline – Identifying the environment in order to identify vulnerabilities and ensure policy compliance
- Prioritization – Using mitigation activities based on external threat information, internal security posture, and asset classification
- Shielding the environment – This is done before eliminating the vulnerability, by using desktop and network security tools
- Mitigation – This is reducing vulnerabilities and eliminating the root causes
- Lifecycle Maintenance – This is maintaining and continually monitoring the environment for deviations from policy and to identify new vulnerabilities

Failure to keep operating system and application software patched is one of the most common issues identified by security and IT professionals. New patches and software upgrades are released daily, and it is often difficult for even experienced system administrators to keep abreast of all the new patches and ensure proper deployment in a timely manner. Most major attacks in the past few years have targeted known vulnerabilities for which patches existed before the outbreaks. Indeed, the moment a patch is released, attackers make a concerted effort to reverse engineer the patch swiftly (measured in days or even hours), identify the vulnerability, and develop and release exploit code. Thus, the time immediately after the release of a patch is ironically a particularly vulnerable moment for most organizations due to the time lag in obtaining, testing, and deploying a patch.

To help address this growing problem, it is recommended that all organizations have a systematic, accountable, and documented process for managing exposure to vulnerabilities through the timely deployment of patches. This includes:

- Vulnerability Assessment – Vulnerability assessment provides baseline and discovery functions in support of vulnerability management. Assessment products scan an endpoint and attempt to determine vulnerable conditions based on a database of known vulnerabilities and can determine many other aspects of the endpoint, including open ports, running services and protocols, applications, and operating system. This information provides security groups with the data they need to measure security postures. When your security group documents the weakness of the network and host infrastructure, you can begin to make decisions on how to eliminate the root cause of the majority of exploits, reduce the potential attack vectors and limit the impact of a security incident.
- Vulnerability Mitigation and Remediation – This includes patching, deleting unauthorized software, closing obvious access paths and/or ports, pushing software updates to servers and user desktops and/or laptops.
- Security Configuration Management and Policy Compliance – Security configuration management and policy compliance tools provide a top-down baseline of the IT environment in relation to an organization's defined security configuration policies. Organizations often define a "gold-standard" environment — the desired state of system configurations and access rights — they can also use a predefined set of best-practice system security configuration templates (such as the Microsoft Security guide, the SANS Institute, the Center for Internet Security, the National Institute of Standards and Technology or the National Security Agency) or vendor-defined templates for regulatory compliance.

- IT Security Risk Management – The primary focus of IT security risk management products is to quantify IT security risk and prioritize/support remediation activities. These products combine asset classification data, embedded security policy functions, current external threat data and the results of third-party VA scans to support aggregated risk analysis and vulnerability mitigation. Security risk management tools provide varying degrees of embedded support for asset classification and security configuration policy management. The analysis produced by these tools attempts to quantify the IT security business risk for resource groups that are aligned to business functions. The products also provide workflow for mitigation, as well as validation that a vulnerability has been eliminated. They also provide the ability to develop an asset repository, classify those assets, generate risk-rating reports, implement remediation workflow and monitor status. Most products in this category integrate assessment data from third-party products, and directly provide varying levels of support for security configuration policy auditing.
- Vulnerability Monitoring – The monitoring step of the vulnerability management process can be automated by regular execution of deployed assessment and security configuration management technologies and through the use of monitoring technology. Monitoring technology provides real-time event management and historical analysis of security data from a wide set of heterogeneous sources. This technology is used to filter incident information into data that can be acted on for the purposes of incident response and forensic analysis. The need to support regulatory compliance has become the new market driver for the technology providers.

Key to establishment and operation of a vulnerability management capability is the people tasked with the effort. The duties of those involved with vulnerability management are:

1. *Create a System Inventory* – The members of the vulnerability management team should use existing inventories of the organization's IT resources to determine which hardware equipment, operating systems, and software applications are used within the organization. The team should also maintain a manual inventory of IT resources not captured in the existing inventories.
2. *Monitor for Vulnerabilities, Remediations, and Threats* – The team is responsible for monitoring security sources for vulnerability announcements, patch and nonpatch remediations, and emerging threats that correspond to the software within the team's system inventory.
3. *Prioritize Vulnerability Remediation* – The team should prioritize the order in which the organization addresses vulnerability remediation.
4. *Create an Organization-Specific Remediation Database* – The team should create a database of remediations that need to be applied throughout the enterprise.
5. *Conduct Generic Testing of Remediations* – The team should be able to test patches and nonpatch remediations on IT devices that use standardized configurations. This will avoid the need for local administrators to perform redundant testing. The team also should work closely with local personnel to test patches and configuration changes on critical systems.
6. *Deploy Vulnerability Remediations* - The team should oversee vulnerability remediation.
7. *Distribute Vulnerability and Remediation Information to Local Administrators* – The team is responsible for informing local administrators about vulnerabilities and remediations that correspond to software packages included within the team scope and that are in the enterprise software inventory.
8. *Perform Automated Deployment of Patches* – The team should deploy patches automatically to IT devices using enterprise patch management tools. Alternately, the team could work closely with the group actually running the patch management tools. Automated patching tools allow an administrator to update hundreds or even thousands of systems from a single console. Deployment is fairly simple when there are homogeneous computing

platforms, with standardized desktop systems and similarly configured servers. Multiplatform environments, nonstandard desktop systems, legacy computers, and computers with unusual configurations may also be integrated.

9. *Configure Automatic Update of Applications Whenever Possible and Appropriate* – Many newer applications provide a feature that checks the vendor's Web-site for updates. This feature can be very useful in minimizing the level of effort required to identify, distribute, and install patches. However, some organizations may not wish to implement this feature because it might interfere with their configuration management process. A recommended option would be a locally distributed automated update process, where the patches are made available from the organization's network. Applications can then be updated from the local network instead of from the Internet.
10. *Verify Vulnerability Remediation Through Network and Host Vulnerability Scanning* – The team should verify that vulnerabilities have been successfully remediated.
11. *Vulnerability Remediation Training* – The team should train administrators on how to apply vulnerability remediations. In enterprises that rely on end users to patch computers, the team also must train users on this function.

STRATEGIES, TOOLS AND TECHNIQUES

VULNERABILITY “WATCH LIST” SERVICES

There are several types of resources available for monitoring the status of vulnerabilities, remediations, and threats. Federal Network Services has created a job aid for its customers that includes a listing of popular resources. Each type of resource has its own strengths and weaknesses. The National Institute for Standards and Technology (NIST) recommends using more than one type of resource to ensure accurate and timely knowledge. The most common types of resources are:

- Vendor Websites and mailing lists
- Third-party Websites
- Third-party mailing lists and newsgroups
- Vulnerability scanners
- Vulnerability databases
- Enterprise patch management tools
- Other notification tools

General industry and government best practice suggests that organizations monitor for vulnerabilities, remediation, and threats using the following resource types at a minimum:

- Enterprise patch management tool, to obtain all available patches from supported vendors
- Vendor security mailing lists and Websites, to obtain all available patches from vendors not supported by the enterprise patch management tool
- Vulnerability database or mailing list to obtain immediate information on all known vulnerabilities and suggested remediations (e.g., the National Vulnerability Database)
- Third-party vulnerability mailing lists that highlight the most critical vulnerabilities (e.g., the US-CERT Cyber Security Alerts). Such lists will help organizations focus on the most important vulnerabilities that may get overlooked among the myriad of vulnerabilities published by more general vulnerability resources.

After initial assessment of a new vulnerability, remediation, or threat, vulnerability management personnel should continue to monitor it for updates and new information. For example, a software vendor might release a new patch in place of a software reconfiguration it originally recommended as a temporary remediation measure. By performing ongoing monitoring for new information, the team will be aware of the new patch and could determine if it would provide a

better solution than the software reconfiguration. Ongoing monitoring is also important because additional analysis of vulnerabilities might determine that they are more or less severe than previously thought.

VULNERABILITY SCANNERS

Vulnerability scanners are commonly used in many organizations to identify vulnerabilities on their hosts and networks. Vulnerability scanners employ large databases of vulnerabilities to identify vulnerabilities associated with commonly used operating systems and applications. There are two types of vulnerability scanners: network scanners and host scanners. Network scanners are used for identifying open ports, vulnerable software, and misconfigured services. Host scanners are used for identifying specific operating system and application misconfigurations and vulnerabilities.

Vulnerability scanners can:

- Proactively identify vulnerabilities
- Provide a fast and easy way to measure exposure
- Automatically fix discovered vulnerabilities
- Identify out-of-date software versions
- Validate compliance with an organizational security policy
- Generate alerts and reports about identified vulnerabilities

However, vulnerability scanners do have some weaknesses. In general, scanners:

- Depend on regular updating of the vulnerability database
- Tend to have a high false positive error rate
- May generate significant amounts of network traffic
- May cause a Denial of Service (DoS) of hosts, because scanner probing may cause a system to crash inadvertently

DEPLOYING VULNERABILITY REMEDIATION

Organizations should deploy vulnerability remediation to all systems that have vulnerabilities, even for systems that are not at immediate risk of exploitation. Vulnerability remediation also should be incorporated into the organization's standard build configurations for hosts and servers. There are three primary methods of remediation that can be applied to an affected system: the installation of a software patch, the adjustment of a configuration setting, and the removal of the affected software.

- *Security Patch Installation* – Applying a security patch (also called a “fix” or “hotfix”) repairs the vulnerability, since patches contain code that modifies the software application to address and eliminate the problem. Patches downloaded from vendor Websites are typically the most up-to-date and are likely free of malicious code.
- *Configuration Adjustment* – Adjusting how an application or security control is configured can effectively block attack vectors and reduce the threat of exploitation. Common configuration adjustments include disabling services and modifying privileges, as well as changing firewall rules and modifying router access controls. Settings of vulnerable software applications can be modified by adjusting file attributes or registry settings.
- *Removal of Unauthorized Software* – Removing or uninstalling the affected software or vulnerable service eliminates the vulnerability and any associated threat. This is a practical solution when an application is not needed on a system. Determining how the system is used, removing unnecessary software and services, and running only what is essential for the system's purpose is a recommended security practice.

The mitigation of vulnerabilities and threats may be as simple as modifying a configuration setting, or as involved as the installation of a completely new version of the software. No simple patch application methodology applies to all software and operating systems. Before performing the remediation, the administrator may want to conduct a full backup of the system to be patched. This will allow for a timely restoration of the system to previous state if the patch has an unintended or unexpected impact on the host.

Applying patches to multiple systems is a constant administrative challenge that may seem especially daunting when implementing patches on hundreds or thousands of servers and desktop systems. This task can be made less burdensome with the use of applications that automatically distribute updates to end-user computers. These enterprise patch management tools are included with network operating system software and distributed by third-party vendors. The capabilities of these tools vary greatly. Some of these tools focus on the distribution of patches, relying on the system administrator to identify a necessary patch and arrange for the tool to deliver and install the patch. Other tools actively search for necessary patches and automatically notify the system administrator of the available ones; the administrator can then approve the tool's installation of the patches on the appropriate hosts. Enterprise management tools can vary greatly in their support of different operating systems and applications. Those that are bundled with an operating system tend to support the fewest operating systems and applications. Those from third-party vendors are generally compatible with the widest range of systems. Automated patch distribution tends to work best for organizations with a relatively homogenous environment and standardized configurations.

Enterprises must apply patches manually for operating systems and applications that their patch management tools do not support. Also, patch management tools cannot update many appliance-based devices; even if the appliances use operating systems and applications that the patch management tools support. This is because appliances often use customized limited-functionality versions of operating systems and applications not intended for administrators to access directly. Because the appliances' customized operating systems and applications are based on the same code as standard programs, they are susceptible to many of the same vulnerabilities. However, appliances often cannot be patched as quickly as standard devices, because appliance patches can be applied only through updates provided by the device's manufacturer. The level of effort needed to apply patches manually for appliances and for operating systems and applications not supported by patch management tools is substantial.

Regardless of whether remediation involves automated patching or manual updates, system administrators may believe that the disadvantages of a suggested remediation outweigh its benefits. They may not wish to install the patches or perform the configuration modifications at all. The reasons behind these decisions should be documented and communicated back to the vulnerability management team and then to the appropriate management for approval.

The risk of delaying remediation must be weighed carefully. Consider:

- *Threat Level* – Does the enterprise or systems that require remediation face numerous and/or significant threats? For example, public Web servers and most Federal government organizations may face heightened threat levels. In general, timely remediation is critical for these systems. In contrast, for an intranet site that is inaccessible from the Internet, remediation can often be delayed because such a site usually faces a lower threat level.
- *Risk of Compromise* – What is the likelihood that a compromise will occur? If the vulnerability is easy to exploit, then remediation should be applied swiftly.
- *Consequences of Compromise* – What are the consequences of compromise? If the system is critical or contains sensitive data, then the remediation should be performed immediately. This holds true even for noncritical systems if a successful exploitation would lead to an attacker gaining full control of the system.

Unfortunately, neither decision—to apply or not apply a remediation—is risk-free. The correct decision is not always clear. The vulnerability management team, system administrators, and enterprise management must work together to create a systematic process for evaluating risks and determining the appropriate decision within the context of their organization.

PERFORMING VULNERABILITY SCANNING

Vulnerability scanners are commonly used in many organizations to identify vulnerabilities on their hosts and networks. A vulnerability scanner identifies not only hosts and open ports on those hosts, but also associated vulnerabilities. A host's operating system and active applications are identified and then compared with a database of known vulnerabilities.

Vulnerability scanners can be of two types:

- Network scanners are used to map an organization's network and identify open ports, vulnerable software, and misconfigured services. They can be installed on a single system on the network and can quickly locate and test numerous hosts. Network scanners are generally ineffective at gathering accurate information on hosts using personal firewalls, unless the personal firewalls are configured to permit the network scanning activity.
- Host scanners must be installed on each host to be tested. These scanners are used primarily to identify specific host operating system and application misconfigurations and vulnerabilities. Host scanners have high detection granularity and usually require not only host (local) access but also a root or administrative account. Some host scanners offer the capability of repairing misconfigurations.

Vulnerability scanners vary widely in capability and performance. Some perform optimized searching and can scan a host or network much faster than other systems. Some provide detailed reports and information about the remediation of each discovered vulnerability, while others only provide the most basic information about which vulnerabilities were found.

Vulnerability scanners employ large databases of vulnerabilities to identify vulnerabilities associated with commonly used operating systems and applications. The vulnerability database must be updated frequently so that the scanners can identify the newest vulnerabilities. When a match is found, the scanner will alert the operator to a possible vulnerability. Most vulnerability scanners also generate reports to help system administrators fix the discovered vulnerabilities. Unfortunately vulnerability scanners are not completely accurate; some vulnerabilities may be missed, and other vulnerabilities that do not exist may be identified. Organizations should consider using multiple vulnerability scanning products so that false positives generated by one scanner can be validated by another.

Vulnerability scanners generally provide the following capabilities:

- Identify active hosts on networks
- Identify active and vulnerable services (ports) on hosts
- Identify vulnerabilities associated with discovered operating systems and applications
- Test compliance with host application usage/security policies

Vulnerability scanners can help identify out-of-date software versions and applicable patches or system upgrades. Vendor products capable of automatically applying remediation based on the user's pre-defined settings and conditions have emerged on the market. Such products are being deployed as security appliances with IT infrastructure. These appliances are becoming more and more capable of automating heretofore, manually intensive and costly functions.

VULNERABILITY REMEDIATION TRAINING

Although the team will monitor for new patches and vulnerabilities found in the enterprise software inventory, local administrators may use other software without prior approval. This

situation results from a management decision that the team has resources only to focus on more popular software packages. In this situation, local administrators should be provided with some knowledge of how to identify new patches and vulnerabilities. Providing such knowledge creates a second line of defense in the patching process. Local administrators should be trained about various vulnerability and patching resources. In addition, all end users expected to implement recommended remediations on their own systems should be educated about the vulnerability management process. This is especially important for remote users.

PROCESS COMPONENTS

Organizations need to create a comprehensive, documented, and accountable process for identifying and addressing vulnerabilities, patches, and threats within an organization. One possible approach is to have a formal, centralized patch and vulnerability group that supports the security efforts of local system administrators.

Specific recommendations for organizations implementing a patch and vulnerability management program are as follows:

- Create an inventory of all information technology assets
- Create a vulnerability management group
- Continuously monitor for vulnerabilities, remediations, and threats
- Prioritize patch application and use phased deployments as appropriate
- Test patches before deployment
- Deploy enterprise-wide automated patching solutions
- Create a remediation database
- Use automatically updating applications as appropriate
- Verify that vulnerabilities have been remediated
- Train applicable staff on vulnerability monitoring and remediation techniques

SUMMARY

Vulnerabilities are assessed through the use of automated tools, some of which provide reporting capabilities based on Federal requirements. INFOSEC Services can use the tools specified by the customer; however when no tool is specified, we recommend the use of Lockdown Networks products as they are the only tools on the market that provide for direct reporting of vulnerabilities on POA&Ms under FISMA.

Federal Network Services' INFOSEC Services practice specializes in providing Information System Security Officers (ISSOs) and Information System Security Engineers (ISSEs) to perform this work and to ensure that related systems (e.g., business workflow processes, configuration management, disaster recovery planning, and training [specifically with regard to annual awareness training]) are integrated seamlessly into strategic planning, architecture, vulnerability and risk management, solutions management, incident response and forensics, and audit and survey management as they apply to INFOSEC.

Federal Network Systems' INFOSEC Services practice provides a holistic approach to INFOSEC in general and specifically to vulnerability management efforts for Government and commercial clients. In addition, INFOSEC Services provides services that offer Return-On-Investment (ROI) features for secure operations of IT systems and provides consulting services for better system protection throughout the life cycle of the system.

For more information, refer to the contact information provided on our Website: www.fnsnet.com and a representative will be happy to provide more information.